

**What is claimed is:**

1. A method of generating a content signature for a signal comprising the steps of:  
dividing the signal into at least one set;  
transforming the set into a frequency-based domain;  
determining features of the transformed set; and  
grouping the features to comprise a content signature of the set.
2. A method according to claim 1, wherein the features comprise perceptually relevant features.
3. A method according to claim 1, wherein the features comprise frequency magnitude peaks.
4. A method according to claim 1, further comprising the step of storing the content signature.
5. A method according to claim 1, wherein the step of grouping comprises one of the steps of hashing the features, mathematically representing the features, and mapping the features.
6. A method according to claim 1, further comprising the step of storing the content signature in a database.
7. A method according to claim 1, further comprising the steps of:  
dividing the signal into a plurality of sets;  
transforming each of the plurality of sets into a frequency-based domain;  
determining features for each of the plurality of transformed sets;

grouping the features per set to comprise a respective signature for each of the sets; and  
linking the respective signatures.

8. A method of resolving a stream of content signatures, the content signatures corresponding to sets of a content item, said method comprising the steps of:  
applying Viterbi decoding according to the stream of content signatures;  
identifying a content item corresponding to the stream; and  
accessing information related to the content item.

9. A method of generating a content signature from compressed data, the compressed data having  $m$  bits, said method comprising the steps of:  
extracting  $n$  of the most significant of the  $m$  bits, where  $m > n$ , and  $n$  and  $m$  are integers; and  
storing the  $n$  bits as the content signature.

10. A method of generating a content signature from a content item comprising the steps:  
in a compressed domain, identifying scaling features of the data; and  
grouping the scaling features to form a content signature.

11. A method of generating a content signature for a signal comprising the steps of:  
dividing the signal into at least one set; and  
identifying perceptual edges of the set, the edges comprising the signature of the set.

12. A method of generating a content signature for a signal comprising the steps of:

applying trellis coded quantization to a data set to find a minimum relationship between the data set; and  
storing the minimum relationship as a signature of the data set.

13. A method according to claim 12, wherein trellis coded quantization can be modeled as a trellis diagram representing the data, and the minimum relationship is the shortest distance through the trellis diagram.

14. A method of deriving a content signature for a content item, the content item comprising a digital watermark embedded therein, the digital watermark comprising at least a grid component, said method comprising the steps of:

decoding the embedded digital watermark from the content item to retrieve the grid component;  
rescaling the content item based on the grid component; and  
deriving a content signature for the content item.

15. The method of claim 14, wherein said rescaling comprises at least one of rotating the content item, scaling the content item and translating the content item.

16. The method of claim 15, wherein the content item comprises one of audio, video and image data.

17. A method of handling a content item, the content item comprising a digital watermark embedded therein, the digital watermark comprising at least a message, said method comprising the steps of:

decoding the digital watermark to obtain the message; and  
deriving a content signature for the content item.

18. The method of claim 17, wherein the message comprises a content distributor identifier to be used to identify the distributor of the content item.

19. The method of claim 18, wherein the content signature is used to identify the content item.

20. The method of claim 19, further comprising the steps of selecting a database for interrogation based on the distributor identifier, and identifying information associated with the content item and stored in the selected database with the content signature.

21. The method of claim 17, wherein the message comprises a content signature.

22. The method of claim 21, further comprising the step of comparing the message content signature with derived content signature.

23. The method of claim 22, further comprising the step of deeming the content item authentic when the message content signature and the derived content signature coincide.

24. The method of claim 17, wherein the message comprises a trigger to indicate that said deriving step should be performed.

25. A method to derive a content signature for a video frame or image comprising the steps of:

identifying an area in the video frame or image;

determining a center of mass of the video frame or image; and

providing a content signature for the video frame or image based at least on the center of mass.

26. The method of claim 25, wherein in the center of mass is determined by identifying edges of the area and then determining a center based on the identified edges.

27. The method of claim 25, wherein the area comprises a plurality of pixels, and wherein in the center of mass is determined by multiplying each pixel's luminescence with its location from a predetermined reference point in the area, summing all pixels, and dividing by the average luminescence of the pixels.

28. The method claim 27, wherein the area comprises a plurality of color planes, and a center of mass is calculated for each color plane.

29. The method of claim 25, further comprise the step detecting edges in the area before said step of determining a center of mass.

30. The method of claim 25, wherein the area comprises an object.

31. The method of claim 25, wherein the area comprises a video frame.

32. A method of generating a fingerprint related to a content item comprising the steps of:

pseudorandomly selecting a segment of the content item; and  
fingerprinting the selected segment of content item.

33. The method of claim 32, wherein the segment is pseudorandomly selected based on a known key.

34. The method of claim 33, wherein the known key comprises a user identifier.

35. The method of claim 32, wherein the fingerprinting comprises at least one of mapping perceptually relevant features, a frequency domain analysis, hashing and a lossy transformation.

36. A method of calculating a content signature from a content item, the content item comprising at least one cue signal, said method comprising the steps of:

sensing the cue signal from the content item; and upon sensing the cue signal, determining a content signature for at least a portion of the content item.

37. The method of claim 36, wherein the content item is video and the cue signal comprises a fade to black indicator.

38. The method of claim 36, wherein the cue signal comprises a pattern of frequency components for the content item.

39. The method of claim 36, wherein the content item is video and the cue signal comprises a contrast of a center of a video frame.

40. The method of claim 36, further comprising the step of determining timing intervals within the content item based on the cue signal.

41. A data management method comprising the step of:  
deriving a content signature from a content item; and  
providing the content signature to a database constructed as content addressable memory (CAM); and  
obtaining data from the database associated with the content signature.

42. The method of claim 42, wherein the data comprises at least one of a URL, IP address and metadata.

43. The method of claim 41, wherein the database includes groups of sub-fingerprints, and the content signature is used interrogate the database to identify a related group of sub-fingerprints.

43. The method of claim 41, wherein the database includes groups of sub-fingerprints, and the content signature is used interrogate the database to identify a related group of sub-fingerprints.